UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/615,278	07/08/2003	John Deaver	C0011/7006	1880

64967 7590 10/31/2006

LAW OFFICES OF PAUL E. KUDIRKA
40 BROAD STREET
SUITE 300
BOSTON, MA 02109

EXAMINER
SHAN, APRIL YING

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 10/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/615,278	**Applicant(s)** DEAVER ET AL.	
	Examiner April Y. Shan	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 July 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 December 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *Oct 9, 2003*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-30 have been examined.

Drawings

2. The replacement drawings were received on 29 December 2004. These drawings are entered in the record.

Specification

3. Examiner is aware of the preliminary amended specification received on 29 December 2004 and it is entered in the record.

Claim Objections

4. Claims 1-30 are objected to because of the following informalities:

For example,

a. Applicant repeatly used (d) in claims 2-5, which is confusing. Please remove or clarify.

b. “Apparatus” on line 1, claim 11 should be “An apparatus”;

c. “unsecure” in claims 1 and 10, should be “unsecured”;

d. “unsecure” in claims 9, 19-20, should be “unsecured”

e. As per **claim 2**, "a scheduled key for the first distribution archive file" recited in line 2. It is unclear whether this is intended to be the same or different as "a scheduled key" recited in line 4, claim 1.

Any claim not specifically addressed, above, is being objected as incorporating the deficiencies of a claim upon which it depends.

Please check the claims 1-30 and correct any informality the Applicant is aware of.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-10, 19-20 and 29-30 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per **claim 1**, Steps (a)-(c) are indefinite loops. According to the claim steps (a)-(c) as iteratively repeated for each distribution archive file in the stream, but it becomes indefinite loop because the loop only decrypted the next distribution archive file in the stream following the first distribution archive file, which it turns out be always the second distributed archive file in the stream. In order to further exam the merits on the claim, examiner assumed there are only two distribution archive files in a stream.

As **per claims 9, 19 and 29**, encrypt the extracted scheduled key at the unsecured site is being recited. However, please note in claim 1, 11 and 21, the Applicant recited using the extracted scheduled key to decrypt the next distribution archive and the encrypted scheduled key was encrypted at the publisher's site before sending to the unsecured site. It made no sense to encrypt the scheduled key at the unsecured site and if so, how the extracted scheduled key can be used to decrypt the next distribution archive? In order to further exam on the merits of the claim, the Examiner assumes it is "decrypt the extracted scheduled key", not "encrypt the extracted scheduled key".

Any claim not specifically addressed, above, is being rejected as incorporating the deficiencies of a claim upon which it depends.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

7. Claims 1-30 are rejected under 35 U.S.C. 102(a) as being anticipated by Shen et al. (WO/2002/100037) (an English translation is provided by U.S. Pub No. 2004/0236956 and the below rejections are cited from the translated U.S. Publication).

As per **claims 1 and 11**, Paragraph [193] and [197] in Shen et al.'s reference disclose a method/apparatus for secure key delivery for decrypting a distribution archive file at an unsecured site ("a decryption key embedded in the content is an excellent method for protecting content by processing the key itself" – e.g. paragraph [193]) that receives a stream of distribution archive files from a publishing site, the method/apparatus comprising: extracting a scheduled key from each distribution archive file in the stream; using the stored scheduled key to decrypt the next distribution archive file in the stream following the distribution archive file from which the scheduled key was extracted; and repeating steps (a) and (b) for each distribution archive file in the stream ("Content decoding for authentication ->key extraction ->next authentication decryption using the key extracted in the previous authentication, executable using a looping rule" – e.g. paragraph [197]).

As per **claims 2 and 12**, Shen et al. discloses a method/apparatus as applied in claims 1 and 11. Shen et al. further discloses receiving a scheduled key for the first distribution archive file in the stream from the publishing site ("A license key received from the server is sent to the IPMP tool memory" – e.g. paragraph [0163] and "a license should be retrieved from a license server over a secure channel during a non-standard user authentication process" – e.g. paragraph [0159]. Please note a license key is corresponding to a scheduled key in the claim).

As per **claims 3 and 13**, Shen et al. discloses a method/apparatus as applied in claims 1 and 11. Shen et al. further discloses encrypting, with a scheduled key, a distribution archive file including a scheduled key for the next distribution archive file in the stream and the plurality of encrypted content files ("...protected content by encryption..." – e.g. paragraph [0005] and "the encryption key is encrypted...and inserted to the IPMP information, and is sent to the terminal with the content stream" – e.g. paragraph [0030], paragraph [0031] and fig. 7).

As per **claims 4 and 14**, Shen et al.'s reference discloses a method/apparatus as applied in claims 1 and 11. Paragraph [0159] in Shen et al.'s reference further discloses encrypting, with a scheduled key, a distribution archive file including the plurality of encrypted content files. Inherently, it teaches a non-encrypted scheduled key for the next distribution archive file by showing the key can be encrypted to achieve even greater security.

As per **claims 5 and 15**, Shen et al. discloses a method/apparatus as applied in claims 1 and 11. Shen et al. further discloses encrypting each digital content document with a key to generate encrypted document content (paragraph [0030] and [0031]); at the publishing site, computing for each document, from the encrypted document content for that document, a document identifier that cannot be derived solely from the encrypted version of the requested document ("creating a content ID and an IPMP Tool list relating to the content..." - e.g. claim 1); at the publishing site, creating a list of document identifier and decryption key pairs ("predetermined table" in paragraph [0028] is corresponding to the list in the claim. "The provider has encrypted content and corresponding decryption key" – e.g. paragraph [0217]); at the publishing site, assembling the encrypted document content for each content document and the key pair list into a distribution archive file (fig. 3 and "...assembling a content stream including the IPMP Tool List flag, then the IPMP Tool List, content ID, and the actual coded content stream"- e.g. claims 1 and 17); and encrypting the distribution archive file with a scheduled key ("encrypting the coded content stream using a data encryption tool or other tool" –e.g. claim 2).

As per **claims 6 and 16**, Shen et al. discloses a method/apparatus as applied in claims 5 and 15. Shen et al. further discloses generating a new scheduled key, encrypting the new scheduled key and including the encrypted scheduled key in the distribution archive file (paragraph [0030])

As per **claims 7 and 17**, Shen et al. discloses a method/apparatus as applied in claims 6 and 16. Shen et al. further discloses wherein the new scheduled key is encrypted using a text string embedded in program code in the publishing site (paragraph [0159] and "is encrypted using an IPMP tool such as DES" – paragraph [0031]. It is well known in the art that DES is a symmetric algorithm and the same key is used for encryption and decryption. Therefore, it is the same key both for encryption and decryption)

As per **claims 8 and 18**, Shen et al. discloses a method/apparatus as applied in claims 7 and 17. Shen et al. further discloses wherein step (a) comprises storing an extracted scheduled key in encrypted form ("An encrypted scrambled key is stored in the IPMP elementary stream 325" – e.g. paragraph [0144]).

As per **claims 9 and 19**, Shen et al. discloses a method/apparatus as applied in claims 8 and 18. Shen et al. further discloses wherein the extracted scheduled key is decrypted with a text string embedded in program code at the unsecured site ("...key used to decrypt the scrambling key for the scrambled content is called the "license." A license retrieved from a license server over a secure channel during a non-standard user authentication process" – paragraph [0159])

As per **claims 10 and 20**, Shen et al. discloses a method/apparatus as applied in claims 9 and 19. Shen et al. further discloses wherein the text string embedded in program code in the publishing site is the same as the text string embedded in program code at the unsecured site ("is encrypted using an IPMP tool such as DES" – paragraph [0031]. It is well known in the art that DES is a symmetric algorithm and the same key is used for encryption and decryption. Therefore, it is the same key both for encryption and decryption)

As per **claims 21-30**, Shen et al. disclosed the claimed method of steps as applied in claims 1-10. Therefore, Shen et al. discloses the claimed computer program embodied in a computer usable medium for carrying out the method of steps.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Morishita (U.S. Patent 7,095,853) discloses a method of preventing illegal copy of contents encrypts a header using a key generated from the previous sector.
- Ogawa et al. (U.S. Patent 5,787,179) discloses a scrambling method of a stream formed of a series of unit streams in succession.
- DiSanto et al. (U.S. Pub No. 2002/0146118) discloses a method and system of alternatively selecting an encryption key used to transmit a known number data bits. The receiving party, having received, and decrypted, a previously transmitted message block has sufficient information to determine the encryption key used to encrypt a subsequent data block and is able to decrypt the subsequently transmitted message.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to April Y. Shan whose telephone number is (571) 270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AYS

24 October 2006
AYS

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100